UNITED STATES DISTRICT COURT

WESTERN DISTRICT OF WASHINGTON

SEATTLE DIVISION

JASON GREGORIO, individually and on behalf of all others similarly situated,

Plaintiff,

v.

GREEN DIAMOND RESOURCE COMPANY,

Defendant.

Case No. 2:24-cv-00596

CLASS ACTION COMPLAINT

DEMAND FOR JURY TRIAL

Plaintiff Jason Gregorio ("Plaintiff"), individually and on behalf of all other similarly situated individuals, and by and through his undersigned counsel files this Class Action Complaint against Defendant Green Diamond Resource Company ("Green Diamond" or "Defendant") and alleges the following based upon his personal knowledge of the facts, upon information and belief, and based upon the investigation of his counsel.

NATURE OF THE ACTION

1. Plaintiff brings this class action lawsuit against Green Diamond for its negligent failure to protect and safeguard Plaintiff's and the Class's highly sensitive personally identifiable information ("PII") culminating in a massive and preventable data breach (the "Data Breach" or

TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53703-3515
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

"Breach"). As a result of Green Diamond's insufficient data security, cybercriminals easily infiltrated Green Diamond's inadequately protected computer systems and stole the PII of Plaintiff and the Class (approximately 27,896 individuals).[1]

2. There is no question Plaintiff's and the Class's PII is in the hands of ill-intentioned cybercriminals, shortly after the Data Breach, well-known ransomware group, Akira, claimed responsibility for the Data Breach and claimed to post approximately 30GB of data stolen in the Breach on the dark web.[2]

Year	Month, Year	Company Affected	Industry	Sub-Industry	City/County	State	# Records Affected	Ransom Paid	Ransom Amount	Ransom Strain
2023	Jun, 2023	Green Diamond Resource Company	Business	Other	Seattle	Washington	27,896	Unknown	Unknown	Akira

3. Plaintiff and the Class Members (as further defined below) have had their personally identifiable information exposed as a result of Green Diamond's inadequately secured computer network. Green Diamond betrayed its obligations to Plaintiff and the other Class Members by failing to properly safeguard and protect their PII, thereby enabling cybercriminals to steal their valuable and sensitive information.

4. For the rest of their lives, Plaintiff and the Class Members will have to deal with the danger of identity thieves possessing and misusing their PII. Plaintiff and Class Members will have to spend time responding to the Breach and are at an immediate and heightened risk of all manners of identity theft as a direct and proximate result of the Data Breach. Plaintiff and Class Members have incurred and will continue to incur damages in the form of, among other things, identity theft, attempted identity theft, lost time and expenses mitigating harms, increased risk of

[1] *See* https://apps.web.maine.gov/online/aeviewer/ME/40/b85029fd-4eeb-4059-b381-65ffe99b1d93.shtml.

[2] *See* https://twitter.com/Comparitech/status/1782351310102069710; https://www.comparitech.com/ransomware-attack-map/.

TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53703-3515
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

harm, damaged credit, deprivation of the value of their PII, and/or additional damages as described below.

5. Plaintiff brings this action individually and on behalf of the Class, seeking remedies including, but not limited to, compensatory damages, reimbursement of out-of-pocket costs, injunctive relief, reasonable attorney fees and costs, and all other remedies this Court deems proper.

I. THE PARTIES

6. Plaintiff **Jason Gregorio** is domiciled in and a citizen of the state of California. Plaintiff received a Notice of Data Breach letter ("Notice Letter") from Green Diamond dated April 19, 2024, informing him that his name, Social Security number, date of birth, and full access credentials were accessed and/or acquired by an unauthorized person.[3]

7. Defendant **Green Diamond Resource Company** is a Washington for Profit Corporation with its principal place of business located at 1301 5TH AVE STE 2700, SEATTLE, WA, 98101-2675. Green Diamond's Registered Agent is GALEN G SCHULER, located at 1301 5TH AVE STE 2700, SEATTLE, WA, 98101-2675.

II. JURISDICTION AND VENUE

8. This Court has diversity jurisdiction over this action under the Class Action Fairness Act (CAFA), 28 U.S.C. § 1332(d), because this is a class action involving more than 100 class members, the amount in controversy exceeds $5,000,000, exclusive of interest and costs, and many members of the class are citizens of states different from Defendant.

9. This Court has personal jurisdiction over Defendant because it is headquartered in and/or operates within this District and regularly transacts business, has agents, and is otherwise within this District.

[3] *See* Ex. 1 (Notice Letter).

TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53703-3515
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

10. Venue is likewise proper as to Defendant in this District because a substantial part of the events or omissions giving rise to the claim occurred in this District. 28 U.S.C. § 1391(b)(2).

III. FACTUAL ALLEGATIONS

A. Green Diamond's Massive and Preventable Data Breach.

11. Green Diamond is a forest stewardship company that owns and manages working forests in nine (9) states throughout the western and southern United States.[4]

12. Green Diamond collected the PII of Plaintiffs and the Class for business and/or employment purposes.

13. By collecting the PII of Plaintiffs and the Class Green Diamond undertook a duty to safeguard and protect Plaintiff's and the Class's PII.

14. According to Green Diamond, on or about June 27, 2023, Green Diamond became aware of suspicious activity in its computer network.[5]

15. After an investigation, Green Diamond determined that an unknown actor gained access to certain parts of its network between June 26, 2023, and June 27, 2023.

16. Green Diamond determined that the following types of PII were impacted by the Data Breach: name, date of birth, medical information, health insurance information, Social Security number, financial account information, driver's license number or state identification number, government-issued identification number, passport number, and full access credentials. Green Diamond is not aware of any attempted or actual misuse of individuals' information.[6]

17. In other words, cybercriminals obtained everything they could possibly want to commit identity theft and fraud.

---

[4] *See* https://www.greendiamond.com/about/.

[5] *See* https://www.greendiamond.com/dataevent.pdf.

[6] Information impacted varied by individual.

TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53703-3515
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

18. Despite learning of the Data Breach in June 2023, Green Diamond waited to notify victims of the Data Breach until April 2024, nearly one (1) year later.[7]

19. The Notice Letter obfuscated the nature of the Breach, stating "Green Diamond is notifying you out of an abundance of caution because although there is no evidence that information relating to you was actually seen by any unauthorized person, the investigation determined that certain information relating to you may have been accessed or acquired by an unknown unauthorized person."

20. Shortly after the Data Breach, well-known ransomware group, Akira, claimed responsibility for the Data Breach, as pictured below:[8]

[7] *See* Ex. 1.

[8] https://twitter.com/Comparitech/status/1782351310102069710; https://www.ransomlook.io/group/Akira.

TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53703-3515
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

21. According to Akira, Green Diamond did not "utter a word for about two weeks after the hack."[9]

2023-07-10 | Green Diamond | Green Diamond is a fifth-generation, family-owned forest products company that owns and manages working forests in nine states throughout the western and southern U.S. Working the forest for so long seems to have taken away the management of this company of their ability to communicate with people. They didn't utter a word for about two weeks after the hack.
We found some interesting data on their network and are posting over 30GB of their business information, including personal information, here.

[9] *Id.*; https://twitter.com/FalconFeedsio/status/1678646129011957767/photo/1.

TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53703-3515
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

22. Akira posted over 30GB of data obtained in the Breach on its dark web portal.[10]

23. Green Diamond's Notice Letter to Plaintiff and the Class failed to mention the perpetrator of the attack, Akira.

24. Trend Micro Research states, "Akira is swiftly becoming one of the fastest-growing ransomware families thanks to its use of double extortion tactics, a ransomware-as-a-service (RaaS) distribution model, and unique payment options."[11]

25. "Akira ransomware was first identified in May of 2023, and in less than a year, it has claimed at least 81 victims."[12]

26. "Akira leverages many common features for their targeting and operations. They operate as ransomwareas-a-service (RaaS), which is to say they focus on the ransomware operations, but partner with other cybercriminals for individual attacks and share the extorted fees. They also conduct double extortion; they steal sensitive data, deploy their ransomware, and then charge two fees. The first fee restores the encrypted systems, and the second fee ensures no leaks of stolen data. They are highly reliant on credential compromise as an infection vector, which provides them initial access into their target networks. Akira also operates a leak site where they publicly post information on their victims. Their targeting includes both Windows and Linux infrastructure, and while organizations in the United States are their focus, their targeting is global. They are also known to target the United Kingdom, Canada, Australia, New Zealand and other countries."[13]

27. "Officials from the FBI, Cybersecurity and Infrastructure Security Agency (CISA), Europol's European Cybercrime Centre (EC3), and the Netherlands' National Cyber

---

[10] *Id.*

[11] https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-akira.

[12] https://www.hhs.gov/sites/default/files/akira-randsomware-analyst-note-feb2024.pdf.

[13] https://www.hhs.gov/sites/default/files/akira-randsomware-analyst-note-feb2024.pdf.

TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53703-3515
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

Security Centre (NCSC-NL) published an advisory [] about [Akira], which has earned about $42 million in ransoms since emerging in March 2023."[14]

28. "Akira ransomware actors have used known Cisco vulnerabilities like CVE-2020-3259 and CVE-2023-20269 to breach organizations through virtual private network (VPN) services that did not have multifactor authentication enabled."[15]

29. Akira is also known to use "use spearphishing campaigns and other tools to breach organizations. Once inside, they typically disable security software as a way to avoid detection while moving laterally."[16]

30. "According to the law enforcement agencies, the ransomware gang uses several different tools to exfiltrate data including FileZilla, WinRAR, AnyDesk and more. 'Akira threat actors do not leave an initial ransom demand or payment instructions on compromised networks, and do not relay this information until contacted by the victim,' the agencies said. 'Ransom payments are paid in Bitcoin to cryptocurrency wallet addresses provided by the threat actors. To further apply pressure, Akira threat actors threaten to publish exfiltrated data on the Tor network, and in some instances have called victimized companies, according to FBI reporting.'"[17]

31. All in all, Green Diamond failed to take the necessary precautions required to safeguard and protect Plaintiff's and the other Class Members' PII from unauthorized disclosure. Green Diamond's actions represent a flagrant disregard of the rights of the Class Members, both as to privacy and property.

[14] https://therecord.media/akira-ransomware-attacked-hundreds-millions.

[15] *Id.*

[16] *Id.*

[17] *Id.*

TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53703-3515
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

B. Plaintiff's Experience.

32. Plaintiff received a Notice Letter from Green Diamond dated April 19, 2024, informing him that his name, Social Security number, date of birth, and full access credentials were accessed and/or acquired by an unauthorized person.[18]

33. By soliciting and accepting Plaintiff Gregorio's PII, Green Diamond agreed to safeguard and protect it from unauthorized access and delete it after a reasonable time.

34. Green Diamond was in possession of Plaintiff Gregorio's PII before, during, and after the Data Breach.

35. Following the Data Breach, Plaintiff Gregorio made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to researching the Data Breach, enrolling in the credit monitoring services Green Diamond provided, reviewing and monitoring his accounts for fraudulent activity, and reviewing his credit reports. In total, Plaintiff Gregorio estimates he has already spent **five (5) hours** responding to the Data Breach.

36. Plaintiff Gregorio will be forced to expend additional time to review his credit reports and monitor his accounts for the rest of his life. This is time, spent at Defendant's direction, which has been lost forever and cannot be recaptured.

37. Plaintiff Gregorio places significant value in the security of his PII and does not readily disclose it. Plaintiff Gregorio entrusted Green Diamond with his PII with the understanding that Green Diamond would keep his information secure and would employ reasonable and adequate data security measures to ensure that his PII would not be compromised.

38. Plaintiff Gregorio has never knowingly transmitted unencrypted PII over the internet or any other unsecured source.

39. As a direct and traceable result of the Data Breach, Plaintiff Gregorio suffered actual injury and damages after his PII was compromised and stolen in the Data Breach,

[18] *See* Ex. 1.

TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53703-3515
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

including, but not limited to: (a) lost time and money related to monitoring his accounts and credit reports for fraudulent activity; (b) loss of privacy due to his PII being accessed and stolen by cybercriminals; (c) loss of the benefit of his bargain because Green Diamond did not adequately protect his PII; (d) emotional distress because identity thieves now possess his first and last name paired with his Social Security number and other sensitive information; (e) imminent and impending injury arising from the increased risk of fraud and identity theft now that his PII has been stolen and published on the dark web; (f) diminution in the value of his PII, a form of intangible property that Green Diamond obtained from Plaintiff Gregorio and/or his medical providers; and (g) other economic and non-economic harm.

40. Plaintiff Gregorio has been and will continue to be at a heightened and substantial risk of future identity theft and its attendant damages for ***years*** to come. This risk is certainly real and impending, and is not speculative, given the highly sensitive nature of the PII stolen in the Data Breach.[19]

41. Knowing that thieves intentionally targeted and stole his PII, and knowing that his PII, including his Social Security number, is now in the hands of cybercriminals has caused Plaintiff Gregorio great anxiety beyond mere worry. Specifically, Plaintiff Gregorio has lost hours of sleep, is in a constant state of stress, is very frustrated, and is in a state of persistent worry now that his PII has been stolen.

42. Plaintiff Gregorio has a continuing interest in ensuring that his PII, which, upon information and belief, remains in the possession of Defendant, is protected and safeguarded from future data breaches. Absent Court intervention, Plaintiff Gregorio's PII will be wholly unprotected and at-risk of future data breaches.

[19] *Id.*

TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53703-3515
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

C. Cybercriminals Will Use the PII Obtained in the Breach to Defraud Plaintiff and the Class.

43. PII is of great value to hackers and cybercriminals, and the data stolen in the Data Breach can and will be used in a variety of sordid ways for criminals to exploit Plaintiff and the Class Members and to profit off their misfortune.

44. Each year, identity theft causes tens of billions of dollars of losses to victims in the United States.[20] For example, with the PII stolen in the Data Breach, including Social Security numbers, identity thieves can open financial accounts, apply for credit, file fraudulent tax returns, commit crimes, create false driver's licenses and other forms of identification and sell them to other criminals or undocumented immigrants, steal government benefits, give breach victims' names to police during arrests, and many other harmful forms of identity theft.[21] These criminal activities have and will result in devastating financial and personal losses to Plaintiff and the Class Members.

45. Social Security numbers are particularly sensitive pieces of personal information. As the Consumer Federation of America explains:

> **Social Security number.** *This is the most dangerous type of personal information in the hands of identity thieves* because it can open the gate to serious fraud, from obtaining credit in your name to impersonating you to get medical services, government benefits, your tax refunds, employment – even using your identity in bankruptcy and other legal matters. It's hard to change your Social Security number and it's not a good idea because it is connected to your life in so many ways.[22]
>
> (Emphasis added.)

---

[20] "Facts + Statistics: Identity Theft and Cybercrime," Insurance Info. Inst., https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime (discussing Javelin Strategy & Research's report "2018 Identity Fraud: Fraud Enters a New Era of Complexity").

[21] *See, e.g.*, Christine DiGangi, *5 Ways an Identity Thief Can Use Your Social Security Number*, Nov. 2, 2017, https://blog.credit.com/2017/11/5-things-an-identity-thief-can-do-with-your-social-security-number-108597/.

[22] *Dark Web Monitoring: What You Should Know*, Consumer Federation of America, Mar. 19, 2019, https://consumerfed.org/consumer_info/dark-web-monitoring-what-you-should-know/.

TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53703-3515
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

46. PII is such a valuable commodity to identity thieves that once it has been compromised, criminals will use it for years.[23]

47. This was a financially motivated Breach, as the only reason the cyber criminals go through the trouble of running a targeted cyberattack against companies like Green Diamond is to get information that they can monetize by selling on the black market for use in the kinds of criminal activity described herein. Indeed, a social security number, date of birth, and full name can sell for $60 to $80 on the digital black market.[24] "[I]f there is reason to believe that your personal information has been stolen, you should assume that it can end up for sale on the dark web."[25]

48. These risks are both certainly impending and substantial. As the Federal Trade Commission ("FTC") has reported, if hackers get access to PII, they ***will*** use it.[26]

49. Hackers may not use the information right away, but this does not mean it will not be used. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [I]n some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information ***may continue for years***. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[27]

---

[23] *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, GAO, July 5, 2007, https://www.gao.gov/assets/270/262904.htmlu.

[24] Michael Kan, *Here's How Much Your Identity Goes for on the Dark Web*, Nov. 15, 2017, https://www.pcmag.com/news/heres-how-much-your-identity-goes-for-on-the-dark-web.

[25] *Dark Web Monitoring: What You Should Know*, Consumer Federation of America, Mar. 19, 2019, https://consumerfed.org/consumer_info/dark-web-monitoring-what-you-should-know/.

[26] Ari Lazarus, *How fast will identity thieves use stolen info?*, FED. TRADE COMM'N (May 24, 2017), https://www.consumer.ftc.gov/blog/2017/05/how-fast-will-identity-thieves-use-stolen-info.

[27] *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown,* GAO, July 5, 2007, https://www.gao.gov/assets/270/262904.htmlu.

TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53703-3515
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

50. For instance, with a stolen Social Security number, which is part of the PII compromised in the Data Breach, someone can open financial accounts, get medical care, file fraudulent tax returns, commit crimes, and steal benefits.[28]

51. The ramifications of Defendant' failure to keep its Class Members' PII secure are long lasting and severe. Once that information is stolen, fraudulent use of that information and damage to victims may continue for years. Fraudulent activity might not show up for six to 12 months or even longer.

52. Further, criminals often trade stolen PII on the "cyber black-market" for years following a breach. Cybercriminals can post stolen PII on the internet, thereby making such information publicly available.

53. Approximately 21% of victims do not realize their identify has been compromised until more than two years after it has happened.[29] This gives thieves ample time to, for example, seek multiple medical treatments under the victim's name. Forty percent of consumers found out they were a victim of medical identity theft only when they received collection letters from creditors for expenses that were incurred in their names.[30]

54. Identity theft victims must spend countless hours and large amounts of money repairing the impact to their credit as well as protecting themselves in the future.[31]

---

[28] *See, e.g.*, Christine DiGangi, *5 Ways an Identity Thief Can Use Your Social Security Number*, Nov. 2, 2017, https://blog.credit.com/2017/11/5-things-an-identity-thief-can-do-with-your-social-security-number-108597/.

[29] *See* Medical ID Theft Checklist, *available at:* https://www.identityforce.com/blog/medical-id-theft-checklist-2.

[30] Experian, *The Potential Damages and Consequences of Medical Identify Theft and Healthcare Data Breaches ("Potential Damages*"), *available at:* https://www.experian.com/assets/data-breach/white-papers/consequences-medical-id-theft-healthcare.pdf.

[31] "Guide for Assisting Identity Theft Victims," Federal Trade Commission, 4 (Sept. 2013), http://www.consumer.ftc.gov/articles/pdf-0119-guide-assisting-id-theft-victims.pdf.

TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53703-3515
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

55. As a direct and proximate result of the Data Breach, Plaintiff and the Class have had their PII exposed, have suffered harm as a result, and have been placed at an imminent, immediate, and continuing increased risk of further harm from fraud and identity theft. Plaintiff and the Class must now take the time and effort to mitigate the actual and potential impact of the Data Breach on their everyday lives, including placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, and closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come. Even more seriously is the identity restoration that Plaintiff and other Class Members must go through, which can include spending countless hours filing police reports, following Federal Trade Commission checklists, and calling financial institutions to cancel fraudulent credit applications, to name just a few of the steps.

56. Plaintiff and the Class have suffered, and continue to suffer, actual harms for which they are entitled to compensation, including:

a. Actual identity theft, including fraudulent credit inquiries and cards being opened in their names;

b. Trespass, damage to, and theft of their personal property including PII;

c. Improper disclosure of their PII;

d. Publication of their PII on the dark web;

e. The imminent and certainly impending injury flowing from potential fraud and identity theft posed by their PII being placed in the hands of criminals and having been already misused;

f. Loss of privacy suffered as a result of the Data Breach, including the harm of knowing cyber criminals have their PII and that identity thieves have already used that information to defraud other victims of the Data Breach;

TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53703-3515
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

g. Ascertainable losses in the form of time taken to respond to identity theft and attempt to restore identity, including lost opportunities and lost wages from uncompensated time off from work;

h. Ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably expended to remedy or mitigate the effects of the Data Breach;

i. Ascertainable losses in the form of deprivation of the value of Plaintiff's and Class members' personal information for which there is a well-established and quantifiable national and international market;

j. The loss of use of and access to their credit, accounts, and/or funds;

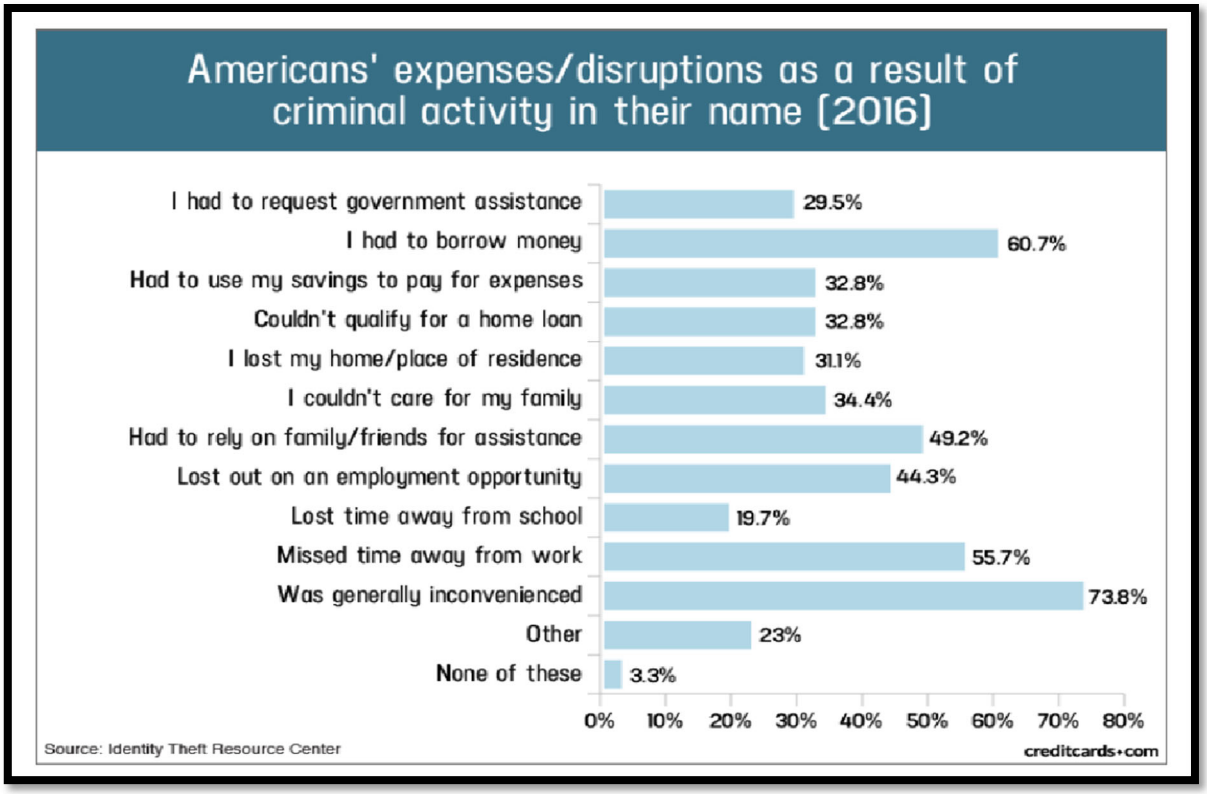
k. Damage to their credit due to fraudulent use of their PII; and

l. Increased cost of borrowing, insurance, deposits, and the inability to secure more favorable interest rates because of a reduced credit score.

57. Below is a chart that shows the kinds of expenses and disruptions that victims of identity theft experience[32]:

[32] Jason Steele, *Credit Card and ID Theft Statistics*, CREDITCARDS.COM (Oct. 24, 2017), https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php.

TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53703-3515
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com



58. Moreover, Plaintiff and Class Members have an interest in ensuring that their information, which remains in the possession of Defendant, is protected from further breaches by the implementation of industry standard security measures and safeguards. Defendant has shown itself wholly incapable of protecting Plaintiff's PII.

59. Plaintiff and Class Members also have an interest in ensuring that their PII that was provided to Green Diamond is removed from Green Diamond's unencrypted files.

60. Defendant itself acknowledged the harm caused by the Data Breach because it offered Plaintiff and Class Members an inadequate 12 or 24 months of identity theft repair and monitoring services. This limited identity theft monitoring is, however, inadequate to protect Plaintiff and Class Members from a lifetime of identity theft risk.[33]

[33] *See* Ex. 1.

TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53703-3515
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

61. Defendant further acknowledged, in its breach notification letter, that, in response to the Data Breach, Green Diamond is "reviewing existing security policies and implemented additional cybersecurity measures to further protect against similar incidents moving forward."[34] Green Diamond should have implemented these additional cybersecurity measures before the Data Breach.

62. The letters further acknowledged that the Data Breach would cause inconvenience to affected individuals by providing numerous actions for Class Members to take in an attempt to mitigate the harm caused by the Data Breach and that financial harm would likely occur. For example, the Green Diamond letter states: "We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors."[35]

63. At Green Diamond's suggestion, Plaintiff is desperately trying to mitigate the damage that Green Diamond has caused him. Given the kind of PII Green Diamond made accessible to hackers, however, Plaintiff is certain to incur additional damages. Because identity thieves have his PII, Plaintiff and all Class Members will need to have identity theft monitoring protection for the rest of their lives. Some may even need to go through the long and arduous process of getting a new Social Security number, with all the loss of credit and employment difficulties that come with a new number.[36]

64. None of this should have happened, the Data Breach was preventable.

D. Defendant were Aware of the Risk of Cyber Attacks

65. Data security breaches have dominated the headlines for the last two decades. And it doesn't take an IT industry expert to know it. The general public can tell you the names of some

---

[34] *Id.*

[35] *Id.*

[36] *Will a New Social Security Number Affect Your Credit?*, LEXINGTON LAW (Nov. 16, 2015), https://www.lexingtonlaw.com/blog/credit-101/will-a-new-social-security-number-affect-your-credit.html.

TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53703-3515
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

of the biggest cybersecurity breaches: Target,[37] Yahoo,[38] Marriott International,[39] Chipotle, Chili's, Arby's,[40] and others.[41]

66. Green Diamond should certainly have been aware, and indeed was aware, that it was at risk for a data breach that could expose the PII that it collected and maintained.

67. It is well-publicized and well-known that Akira is targeting businesses such as Green Diamond.[42]

68. "'The Akira ransomware gang has attacked more than 250 organizations over the last year and continues to impact a "wide range of businesses and critical infrastructure entities in North America, Europe, and Australia,' the FBI and European law enforcement agencies warned[.]"[43]

69. "The ransomware gang has claimed a steady stream of incidents in 2024, including an attack on prominent cloud hosting services provider Tietoevry."[44]

---

[37] Michael Kassner, *Anatomy of the Target Data Breach: Missed Opportunities and Lessons Learned*, ZDNET (Feb. 2, 2015), https://www.zdnet.com/article/anatomy-of-the-target-data-breach-missed-opportunities-and-lessons-learned/.

[38] Martyn Williams, *Inside the Russian Hack of Yahoo: How They Did It*, CSOONLINE.COM (Oct. 4, 2017), https://www.csoonline.com/article/3180762/inside-the-russian-hack-of-yahoo-how-they-did-it.html.

[39] Patrick Nohe, *The Marriot Data Breach: Full Autopsy*, THE SSL STORE: HASHEDOUT (Mar. 22, 2019), https://www.thesslstore.com/blog/autopsying-the-marriott-data-breach-this-is-why-insurance-matters/.

[40] Alfred Ng, *FBI Nabs Alleged Hackers in Theft of 15M Credit Cards from Chipotle, Others*, CNET (Aug. 1, 2018), https://www.cnet.com/news/fbi-nabs-alleged-hackers-in-theft-of-15m-credit-cards-from-chipotle-others/?ftag=CMG-01-10aaa1b.

[41] *See, e.g.*, Taylor Armerding, *The 18 Biggest Data Breaches of the 21st Century*, CSO ONLINE (Dec. 20, 2018), https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html.

[42] *See* https://thehackernews.com/2024/04/akira-ransomware-gang-extorts-42.html; https://thehackernews.com/2024/04/akira-ransomware-gang-extorts-42.html.

[43] https://therecord.media/akira-ransomware-attacked-hundreds-millions.

[44] *Id.*

TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53703-3515
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

70. Green Diamond was clearly aware of the risks and the harm that could result from inadequate date security, but failed to implement appropriate data security measures.

E. Defendant Could Have Prevented the Data Breach.

71. Data breaches are preventable.[45] As Lucy Thompson wrote in the DATA BREACH AND ENCRYPTION HANDBOOK, "In almost all cases, the data breaches that occurred could have been prevented by proper planning and the correct design and implementation of appropriate security solutions."[46] She added that "[o]rganizations that collect, use, store, and share sensitive personal data must accept responsibility for protecting the information and ensuring that it is not compromised . . . ."[47]

72. "Most of the reported data breaches are a result of lax security and the failure to create or enforce appropriate security policies, rules, and procedures. . . . Appropriate information security controls, including encryption, must be implemented and enforced in a rigorous and disciplined manner so that a *data breach never occurs*."[48]

73. In a Data Breach like this, many failures laid the groundwork for the Breach. The FTC has published guidelines that establish reasonable data security practices for businesses. The FTC guidelines emphasize the importance of having a data security plan, regularly assessing risks to computer systems, and implementing safeguards to control such risks.[49] The guidelines establish that businesses should protect the confidential information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies for installing

---

[45] Lucy L. Thomson, "Despite the Alarming Trends, Data Breaches Are Preventable," *in* DATA BREACH AND ENCRYPTION HANDBOOK (Lucy Thompson, ed., 2012).

[46] *Id.* at 17.

[47] *Id.* at 28.

[48] *Id.*

[49] FTC, *Protecting Personal Information: A Guide for Business*, https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53703-3515
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

vendor-approved patches to correct security problems. The guidelines also recommended that businesses utilize an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating hacking attempts; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

74. Upon information and belief, Green Diamond failed to maintain many reasonable and necessary industry standards necessary to prevent a data breach, including the FTC's guidelines. Upon information and belief, Green Diamond also failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework, NIST Special Publications 800-53, 53A, or 800-171; the Federal Risk and Authorization Management Program (FEDRAMP); or the Center for Internet Security's Critical Security Controls (CIS CSC), which are well respected authorities in reasonable cybersecurity readiness.

75. As explained by the Federal Bureau of Investigation, "[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection."[50]

76. To prevent and detect malware attacks, including the malware attack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the Federal Bureau of Investigation, the following measures:

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.
- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.
- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configure firewalls to block access to known malicious IP addresses.

[50] *See* How to Protect Your Networks from RANSOMWARE, at 3, *available at* https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view.

TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53703-3515
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.
- Set anti-virus and anti-malware programs to conduct regular scans automatically.
- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.
- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.
- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.
- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.
- Consider disabling Remote Desktop protocol (RDP) if it is not being used.
- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.
- Execute operating system environments or specific programs in a virtualized environment.
- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.[51]

77. Further, to prevent and detect malware attacks, including the malware attack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the United States Cybersecurity & Infrastructure Security Agency, the following measures:

[51] *Id.* at 3–4.

TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53703-3515
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

- **Update and patch your computer**. Ensure your applications and operating systems (OSs) have been updated with the latest patches. Vulnerable applications and OSs are the target of most ransomware attacks….

- **Use caution with links and when entering website addresses**. Be careful when clicking directly on links in emails, even if the sender appears to be someone you know. Attempt to independently verify website addresses (e.g., contact your organization's helpdesk, search the internet for the sender organization's website or the topic mentioned in the email). Pay attention to the website addresses you click on, as well as those you enter yourself. Malicious website addresses often appear almost identical to legitimate sites, often using a slight variation in spelling or a different domain (e.g., .com instead of .net)….

- **Open email attachments with caution**. Be wary of opening email attachments, even from senders you think you know, particularly when attachments are compressed files or ZIP files.

- **Keep your personal information safe**. Check a website's security to ensure the information you submit is encrypted before you provide it….

- **Verify email senders**. If you are unsure whether or not an email is legitimate, try to verify the email's legitimacy by contacting the sender directly. Do not click on any links in the email. If possible, use a previous (legitimate) email to ensure the contact information you have for the sender is authentic before you contact them.

- **Inform yourself**. Keep yourself informed about recent cybersecurity threats and up to date on ransomware techniques. You can find information about known phishing attacks on the Anti-Phishing Working Group website. You may also want to sign up for CISA product notifications, which will alert you when a new Alert, Analysis Report, Bulletin, Current Activity, or Tip has been published.

- **Use and maintain preventative software programs**. Install antivirus software, firewalls, and email filters—and keep them updated—to reduce malicious network traffic….[52]

78. In addition, to prevent and detect ransomware attacks, including the ransomware attack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

[52] *See* Security Tip (ST19-001) Protecting Against Ransomware (original release date Apr. 11, 2019), *available at* https://us-cert.cisa.gov/ncas/tips/ST19-001.

TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53703-3515
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

- **Secure internet-facing assets**
  - Apply latest security updates
  - Use threat and vulnerability management
  - Perform regular audit; remove privileged credentials
- **Thoroughly investigate and remediate alerts**
  - Prioritize and treat commodity malware infections as potential full compromise;
- **Include IT Pros in security discussions**
  - Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;
- **Build credential hygiene**
  - Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords
- **Apply principle of least-privilege**
  - Monitor for adversarial activities
  - Hunt for brute force attempts
  - Monitor for cleanup of Event Logs
  - Analyze logon events
- **Harden infrastructure**
  - Use Windows Defender Firewall
  - Enable tamper protection
  - Enable cloud-delivered protection
  - Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].[53]

[53] *See* Human-operated ransomware attacks: A preventable disaster (Mar 5, 2020), *available at* https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/.

TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53703-3515
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

79. Given that Defendant was storing the PII of many individuals, Defendant could and should have implemented all of the above measures to prevent and detect ransomware attacks.

80. Specifically, among other failures, Green Diamond had far too much confidential unencrypted information held on its systems. Such PII should have been segregated into an encrypted system.[54]

81. In sum, this Data Breach could have readily been prevented through the use of industry standard network segmentation and encryption of all confidential information. Further, the Data Breach could have likely been prevented had Defendant utilized appropriate malware prevention and detection technologies.

82. Green Diamond was negligent in its failure to ensure it had proper security measures in place to store Plaintiff's and Class Members' confidential PII.

F. Defendant's Response to the Data Breach is Inadequate.

83. Defendant failed to inform Plaintiff and Class Members of the Data Breach in time for them to protect themselves from identity theft.

84. Defendant stated that the Data Breach was discovered in or around June 2023—months after Defendant notified Plaintiffs and the Class of the Data Breach. Even then, Defendant failed to inform Plaintiff and Class Members exactly what information was exposed in the Data Breach, leaving Plaintiff and Class Members unsure as to the scope of information that was compromised.

85. During these intervals, the cybercriminals were exploiting the information while Green Diamond was secretly still investigating the Data Breach.

[54] *See, e.g.,* Adnan Raja, *How to Safeguard Your Business Data with Encryption*, Aug. 14, 2018, https://digitalguardian.com/blog/how-safeguard-your-business-data-encryption.

TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53703-3515
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

86. If Green Diamond had investigated the Data Breach more diligently and reported it sooner, Plaintiff and the Class could have taken steps to protect themselves sooner and to mitigate the damages caused by the Breach.

IV. CLASS ACTION ALLEGATIONS

87. Plaintiff incorporates by reference all preceding paragraphs as if fully restated herein.

88. Plaintiff brings this action against Green Diamond and Green Diamond on behalf of themselves and all other individuals similarly situated under Federal Rule of Civil Procedure 23. Plaintiff asserts all claims on behalf of a nationwide class and the state subclass (collectively, the "Class") defined as follows:

Nationwide Class
All persons whose PII was compromised as a result of the Data Breach.

California Subclass
All persons residing in California whose PII was compromised as a result of the Data Breach.

89. Excluded from the Class is Defendant, any entity in which Defendant has a controlling interest, and Defendant's officers, directors, legal representatives, successors, subsidiaries, and assigns. Also excluded from the Class is any judge, justice, or judicial officer presiding over this matter and members of their immediate families and judicial staff.

90. Plaintiff reserves the right to amend the above definitions or to propose additional subclasses in subsequent pleadings and motions for class certification.

91. The proposed Class meets the requirements of Fed. R. Civ. P. 23(a), (b)(1), (b)(2), (b)(3), and (c)(4).

92. **Numerosity:** The proposed Class is so numerous that joinder of all members is impracticable. The class is comprised of over 27,000 people.

93. **Typicality:** Plaintiff's claims are typical of the claims of the Class. Plaintiff and all members of the Class were injured through Green Diamond's uniform misconduct. The same

TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53703-3515
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

event and conduct that gave rise to Plaintiff's claims are identical to those that give rise to the claims of every other Class member because Plaintiff and each member of the Class had their sensitive PII compromised in the same way by the same conduct of Green Diamond.

94. **Adequacy:** Plaintiff is an adequate representative of the Class because Plaintiff's interests do not conflict with the interests of the Class; Plaintiff has retained counsel competent and highly experienced in data breach class action litigation; and Plaintiff and Plaintiff's counsel intend to prosecute this action vigorously. The interests of the Class will be fairly and adequately protected by Plaintiff and his counsel.

95. **Superiority:** A class action is superior to other available means of fair and efficient adjudication of the claims of Plaintiff and the Class. The injury suffered by each individual class member is relatively small in comparison to the burden and expense of individual prosecution of complex and expensive litigation. It would be very difficult if not impossible for members of the Class individually to effectively redress Green Diamond's wrongdoing. Even if Class members could afford such individual litigation, the court system could not. Individualized litigation presents a potential for inconsistent or contradictory judgments. Individualized litigation increases the delay and expense to all parties, and to the court system, presented by the complex legal and factual issues of the case. By contrast, the class action device presents far fewer management difficulties and provides benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

96. **Commonality and Predominance:** There are many questions of law and fact common to the claims of Plaintiff and the other members of the Class, and those questions predominate over any questions that may affect individual members of the Class. Common questions for the Class include:

a. Whether Defendant engaged in the wrongful conduct alleged herein;

b. Whether Defendant failed to adequately safeguard Plaintiff's and the Class's PII;

TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53703-3515
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

c. Whether Defendant owed a duty to Plaintiff and the Class to adequately protect their PII, and whether it breached this duty;

d. Whether Defendant breached their duties to Plaintiff and the Class as a result of the Data Breach;

e. Whether Defendant failed to provide adequate cyber security;

f. Whether Defendant knew or should have known that its computer and network security systems were vulnerable to cyber attacks;

g. Whether Defendant conduct, including their failure to act, resulted in or was the proximate cause of the breach of its company network;

h. Whether Green Diamond was negligent in permitting unencrypted PII of vast numbers of individuals to be stored within its network;

i. Whether Green Diamond was negligent in permitting unencrypted PII of vast numbers of individuals to be stored within Green Diamond's network;

j. Whether Defendant were negligent in failing to adhere to reasonable retention policies, thereby greatly increasing the size of the Data Breach to include former employees, applicants, and business associates;

k. Whether Defendant failed to adequately respond to the Data Breach, including failing to investigate it diligently and notify affected individuals in the most expedient time possible and without unreasonable delay, and whether this caused damages to Plaintiff and the Class;

l. Whether Green Diamond continues to breach duties to Plaintiff and the Class;

m. Whether Plaintiff and the Class suffered injury as a proximate result of Defendant' negligent actions or failures to act;

n. Whether Plaintiff and the Class are entitled to recover damages, equitable relief, and other relief; and

TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53703-3515
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

o. Whether Defendant' actions alleged herein constitute gross negligence, and whether Plaintiff and Class Members are entitled to punitive damages.

V. CAUSES OF ACTION

FIRST CAUSE OF ACTION
NEGLIGENCE
(On Behalf of all Plaintiff and the Class)

97. Plaintiff incorporates by reference all preceding factual allegations as though fully alleged here.

98. Defendant Green Diamond solicited, gathered, and stored the PII of Plaintiff and the Class.

99. Defendant had full knowledge of the sensitivity of the PII it maintained and of the types of harm that Plaintiff and Class Members could and would suffer if their PII were wrongfully disclosed. Defendant had a duty to Plaintiff and each Class Member to exercise reasonable care in holding, safeguarding, and protecting that information. Plaintiff and the Class Members were the foreseeable victims of any inadequate safety and security practices. Plaintiff and the Class Members had no ability to protect their PII that was in Green Diamond's possession. As such, a special relationship existed between Green Diamond and the Plaintiff and the Class.

100. Defendant was well aware of the fact that cybercriminals routinely target organizations through cyberattacks in an attempt to steal the collected PII.

101. Defendant owed Plaintiff and the Class Members a common law duty to use reasonable care to avoid causing foreseeable risk of harm to Plaintiff and the Class when obtaining, storing, using, and managing PII, including taking action to reasonably safeguard such data and providing notification to Plaintiff and the Class Members of any breach in a timely manner so that appropriate action could be taken to minimize losses.

102. Defendant's duties extended to protecting Plaintiff and the Class from the risk of foreseeable criminal conduct of third parties, which has been recognized in situations where the

TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53703-3515
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

actor's own conduct or misconduct exposes another to the risk or defeats protections put in place to guard against the risk, or where the parties are in a special relationship. *See* Restatement (Second) of Torts § 302B.

103. Defendant had duties to protect and safeguard the PII of Plaintiff and the Class from being vulnerable to cyberattacks, including, by encrypting documents containing PII, by not permitting documents containing unencrypted PII to be maintained on its systems, and other similarly common-sense precautions when dealing with sensitive PII. Additional duties that Green Diamond owed Plaintiff and the Class include:

a. To exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting the PII in its possession;

b. To protect the PII in its possession using reasonable and adequate security procedures and systems;

c. To adequately and properly audit and test its systems;

d. To adequately and properly audit, test, and train its employees regarding how to properly and securely transmit and store PII;

e. To adequately and properly audit, test, and train its employees regarding how to avoid phishing attempts and scams;

f. To train its employees not to store PII for longer than absolutely necessary;

g. To implement processes to quickly detect a data breach, security incident, or intrusion; and

h. To promptly notify Plaintiff and Class Members of any data breach, security incident, or intrusion that affected or may have affected their PII.

104. Plaintiff and the Class were the intended beneficiaries of Defendant's duties, creating special relationships between them and Green Diamond. Defendant was in a position to ensure that its systems were sufficient to protect the PII that Plaintiff and the Class had entrusted to it.

TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53703-3515
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

105. Defendant breached its duties of care by failing to adequately protect Plaintiff's and Class Members' PII. Defendant breached its duties by, among other things:

a. Failing to exercise reasonable care in obtaining, retaining securing, safeguarding, deleting, and protecting the PII in its possession;

b. Failing to protect the PII in its possession using reasonable and adequate security procedures and systems;

c. Failing to adequately and properly audit and test its computer systems to avoid cyberattacks;

d. Failing to adequately and properly audit, test, and train its employees regarding how to properly and securely transmit and store PII, including maintaining it in an encrypted format;

e. Failing to adequately and properly audit, test, and train its employees regarding how to avoid phishing attempts and scams

f. Failing to consistently enforce security policies aimed at protecting Plaintiff and the Class's PII;

g. Failing to implement processes to quickly detect data breaches, security incidents, or intrusions;

h. Failing to abide by reasonable retention and destruction policies for PII it collects and stores; and

i. Failing to promptly and accurately notify Plaintiff and Class Members of the Data Breach that affected their PII.

106. Defendants' willful failures to abide by these duties was wrongful, reckless, and grossly negligent in light of the foreseeable risks and known threats.

107. As a proximate and foreseeable result of Defendant's grossly negligent conduct, Plaintiff and the Class have suffered damages and are at imminent risk of additional harms and damages (as alleged above).

TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53703-3515
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

108. The damages Plaintiff and the Class have suffered (as alleged above) were and are reasonably foreseeable.

109. The damages Plaintiff and the Class have and will suffer were and are the direct and proximate result of Defendant's grossly negligent conduct.

110. Plaintiff and the Class have suffered injury, including as described above, and are entitled to actual and punitive damages in an amount to be proven at trial.

SECOND CAUSE OF ACTION
UNJUST ENRICHMENT
(On Behalf of Plaintiff and the Class)

111. Plaintiff incorporates by reference all preceding factual allegations as though fully alleged here.

112. Through the use of Plaintiff's and Class Members' PII, Defendant received monetary benefits.

113. Defendant collected, maintained, and stored the PII of Plaintiff and Class Members and, as such, Defendant had direct knowledge of the monetary benefits conferred upon it by Plaintiff and Class Members.

114. Defendant appreciated that a monetary benefit was being conferred upon it by Plaintiff and Class Members and accepted that monetary benefit.

115. However, acceptance of the benefit under the facts and circumstances described herein, make it inequitable for Defendant to retain that benefit without payment of the value thereof. Specifically, Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiff's and Class Members' PII. Instead of providing a reasonable level of security that would have prevented the Data Breach, Green Diamond instead calculated to increase its own profits at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective security measures. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's decision to prioritize its own profits over the requisite data security.

TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53703-3515
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

116. Under the principle of equity and good conscience, Defendant should not be permitted to retain the monetary benefit belonging to Plaintiff and Class Members because Green Diamond failed to implement the appropriate data management and security measures, and Green Diamond failed to ensure the appropriate data management and security measures were in place.

117. Defendant acquired the PII through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

118. If Plaintiff and Class Members knew that Defendant had not secured their PII, they would not have agreed to allow Defendant to have or maintain their PII.

119. As a direct and proximate result of Green Diamond's decision to profit rather than provide adequate data security, and as a direct and proximate cause of Green Diamond's failure to ensure it provided adequate data security, Plaintiff and Class members suffered and continue to suffer actual damages, including (i) the amount of the savings and costs Green Diamond reasonably should have expended on data security measures to secure Plaintiff's PII, (ii) time and expenses mitigating harms, (iii) diminished value of the PII, (iv) harms as a result of identity theft; and (v) an increased risk of future identity theft.

120. Defendant, upon information and belief, has therefore engaged in opportunistic, unethical, and immoral conduct by profiting from conduct that it knew would create a significant and highly likely risk of substantial and certainly impending harm to Plaintiff and the Class in direct violation of Plaintiff's and Class members' legally protected interests. As such, it would be inequitable, unconscionable, and unlawful to permit Defendant to retain the benefits it derived as a consequence of its wrongful conduct.

121. Accordingly, Plaintiff and the Class are entitled to relief in the form of restitution and disgorgement of all ill-gotten gains, which should be put into a common fund to be distributed to Plaintiff and the Class.

TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53703-3515
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

THIRD CAUSE OF ACTION
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiff and the Class)

122. Plaintiff incorporates by reference all allegations of the preceding factual allegations as though fully set forth herein.

123. Defendant required Plaintiff and Class Members to provide services and/or employment. In exchange, Defendant entered into implied contracts with Plaintiff and Class Members in which Defendant agreed to comply with its statutory and common law duties to protect Plaintiff's and Class members' PII and to timely notify them in the event of a data breach.

124. Plaintiff and Class Members would not have provided their PII to Defendant had they known that Defendant would not safeguard their PII, as promised, or provide timely notice of a data breach.

125. Plaintiff and Class Members fully performed their obligations under their implied contracts with Defendant.

126. Defendant breached the implied contracts by failing to safeguard Plaintiff's and Class members' PII and by failing to provide them with timely and accurate notice of the Data Breach.

127. The losses and damages Plaintiff and Class members sustained (as described above) were the direct and proximate result of Defendant's breach of its implied contracts with Plaintiff and Class members.

FOURTH CAUSE OF ACTION
VIOLATION OF CALIFORNIA'S UNFAIR COMPETITION LAW ("UCL")
Cal. Bus. & Prof. Code § 17200, *et seq*.
(On Behalf of Plaintiff and the California Subclass)

128. Plaintiff incorporates by reference all preceding factual allegations as though fully alleged here.

129. Plaintiff brings this Count on his own behalf and on behalf of the California Subclass.

TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53703-3515
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

130. The UCL prohibits any "unlawful" or "unfair" business act or practice, as those terms are defined by the UCL and relevant case law. By virtue of the above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach, Defendant engaged in unlawful and unfair practices within the meaning, and in violation, of the UCL.

131. In the course of conducting its business, Defendant committed "unlawful" business practices by, inter alia, knowingly failing to design, adopt, implement, control, direct, oversee, manage, monitor and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect Plaintiff's and California Subclass members' PII, and by violating the statutory and common law alleged herein, including, *inter alia*, the California Consumer Privacy Act of 2018 (Cal. Civ. Code § 1798.100, *et seq.*), Article I, Section 1 of the California Constitution (California's constitutional right to privacy), Cal. Civil Code § 1798.81.5, 45 C.F.R. § 164, *et seq.*, and Section 5 of the FTC Act. Plaintiff and California Subclass members reserve the right to allege other violations of law by Defendant constituting other unlawful business acts or practices. Defendant's above-described wrongful actions, inaction, omissions, and want of ordinary care are ongoing and continue to this date.

132. Defendant also violated the UCL by failing to timely notify Plaintiff and California Subclass members pursuant to Civil Code § 1798.82(a) regarding the unauthorized access and disclosure of their PII. If Plaintiff and California Subclass members had been notified in an appropriate fashion, they could have taken precautions to safeguard and protect their PII and identities.

133. Defendant violated the unfair prong of the UCL by establishing the sub-standard security practices and procedures described herein; by soliciting and collecting Plaintiff's and California Subclass members' PII with knowledge that the information would not be adequately protected; and by storing Plaintiff's and California Subclass members' PII in an unsecure

TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53703-3515
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

electronic environment. These unfair acts and practices were immoral, unethical, oppressive, unscrupulous, unconscionable, and/or substantially injurious to Plaintiff and California Subclass members. They were likely to deceive the public into believing their PII was securely stored when it was not. The harm these practices caused to Plaintiff and California Subclass members outweighed their utility, if any.

134. Defendant's above-described wrongful actions, inaction, omissions, want of ordinary care, misrepresentations, practices, and non-disclosures also constitute "unfair" business acts and practices in violation of the UCL in that Defendant's wrongful conduct is substantially injurious to consumers, offends legislatively-declared public policy, and is immoral, unethical, oppressive, and unscrupulous. Defendant's practices are also contrary to legislatively declared and public policies that seek to protect PII and ensure that entities who solicit or are entrusted with personal data utilize appropriate security measures, as reflected by laws such as the CCPA and the FTC Act (15 U.S.C. § 45). The gravity of Defendant's wrongful conduct outweighs any alleged benefits attributable to such conduct. There were reasonably available alternatives to further Defendant's legitimate business interests other than engaging in the above-described wrongful conduct.

135. Plaintiff and California Subclass members suffered injury in fact and lost money or property as a result of Defendant's violations of statutory and common law. Plaintiff and the California Subclass suffered from overpaying for services that should have included adequate data security for their PII, by experiencing a diminution of value in their PII as a result if its theft by cybercriminals, the loss of Plaintiff's and California Subclass members' legally protected interest in the confidentiality and privacy of their PII, and additional losses as described above.

136. Plaintiff and California Subclass members have also suffered (and will continue to suffer) economic damages and other injury and actual harm in the form of, *inter alia*, (i) an imminent, immediate and the continuing increased risk of identity theft and identity fraud—risks justifying expenditures for protective and remedial services for which they are entitled to

TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53703-3515
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

compensation, (ii) invasion of privacy, (iii) breach of the confidentiality of their PII, (iv) deprivation of the value of their PII for which there is a well-established national and international market, and/or (v) the financial and temporal cost of monitoring their credit, monitoring financial accounts, and mitigating damages.

137. Unless restrained and enjoined, Defendant will continue to engage in the above-described wrongful conduct and more data breaches will occur. As such, Plaintiff, on behalf of herself and California Subclass members, seeks restitution and an injunction, including public injunctive relief prohibiting Defendant from continuing such wrongful conduct, and requiring Defendant to modify its corporate culture and design, adopt, implement, control, direct, oversee, manage, monitor and audit appropriate data security processes, controls, policies, procedures protocols, and software and hardware systems to safeguard and protect the PII entrusted to it, as well as all other relief the Court deems appropriate, consistent with Bus. & Prof. Code § 17203. To the extent any of these remedies are equitable, Plaintiff and the Class seek them in the alternative to any adequate remedy at law they may have.

FIFTH CAUSE OF ACTION
VIOLATION OF THE WASHINGTON CONSUMER PROTECTION ACT
(On Behalf of Plaintiff and the Class)

138. Plaintiff incorporates by reference all preceding factual allegations as though fully alleged here

139. The Washington State Consumer Protection Act, RCW 19.86.020 (the "CPA") prohibits any "unfair or deceptive acts or practices" in the conduct of any trade or commerce as those terms are described by the CPA and relevant case law.

140. Defendant is a "person" as described in RWC 19.86.010(1).

141. Defendant engages in "trade" and "commerce" as described in RWC 19.86.010(2) in that it engages in the sale of services and commerce directly and indirectly affecting the people of the State of Washington.

TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53703-3515
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

142. By virtue of the above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach, Defendant engaged in unlawful, unfair and fraudulent practices within the meaning, and in violation of, the CPA, in that Defendant's practices were injurious to the public interest because they injured other persons, had the capacity to injure other persons, and have the capacity to injure other persons.

143. In the course of conducting their business, Defendant committed "unfair or deceptive acts or practices" by, *inter alia*, knowingly failing to design, adopt, implement, control, direct, oversee, manage, monitor and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect Plaintiff's and Class Members' PII, and violating the common law alleged herein in the process. Plaintiff and Class Members reserve the right to allege other violations of law by Defendant constituting other unlawful business acts or practices. As described above, Defendant's wrongful actions, inaction, omissions, and want of ordinary care are ongoing and continue to this date.

144. Defendant also violated the CPA by failing to timely notify and concealing from Plaintiff and Class Members information regarding the unauthorized release and disclosure of their PII. If Plaintiff and Class Members had been notified in an appropriate fashion, and had the information not been hidden from them, they could have taken precautions to safeguard and protect their PII, medical information, and identities.

145. Defendant's above-described wrongful actions, inaction, omissions, want of ordinary care, misrepresentations, practices, and non-disclosures also constitute "unfair or deceptive acts or practices" in violation of the CPA in that Defendant's wrongful conduct is substantially injurious to other persons, had the capacity to injure other persons, and has the capacity to injure other persons.

146. The gravity of Defendant's wrongful conduct outweighs any alleged benefits attributable to such conduct. There were reasonably available alternatives to further Defendant's legitimate business interests other than engaging in the above-described wrongful conduct.

TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53703-3515
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

147. As a direct and proximate result of Defendant's above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach and their violations of the CPA, Plaintiff and Class Members have suffered, and will continue to suffer, economic damages and other injury and actual harm in the form of, inter alia, (1) an imminent, immediate and the continuing increased risk of identity theft, identity fraud and medical fraud—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (2) invasion of privacy; (3) breach of the confidentiality of their PII; (5) deprivation of the value of their PII, for which there is a well-established national and international market; and/or (6) the financial and temporal cost of monitoring credit, monitoring financial accounts, and mitigating damages.

148. Unless restrained and enjoined, Defendant will continue to engage in the above-described wrongful conduct and more data breaches will occur. Plaintiff, therefore, on behalf of themselves and the Class, seek restitution and an injunction prohibiting Defendant from continuing such wrongful conduct, and requiring Defendant to design, adopt, implement, control, direct, oversee, manage, monitor and audit appropriate data security processes, controls, policies, procedures protocols, and software and hardware systems to safeguard and protect the PII entrusted to it.

149. Plaintiff, on behalf of himself and Class Members, also seeks to recover actual damages sustained by each Class Member together with the costs of the suit, including reasonable attorney fees. In addition, Plaintiff, on behalf of himself and Class Members, request that this Court use its discretion, pursuant to RCW 19.86.090, to increase the damages award for each Class Member by three times the actual damages sustained not to exceed $25,000.00 per Class Member.

TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53703-3515
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

SIXTH CAUSE OF ACTION
INJUNCTIVE AND DECLARATORY RELIEF
(On Behalf of Plaintiff and the Class)

150. Plaintiff incorporates by reference all preceding factual allegations as though fully alleged here.

151. This count is brought under the Federal Declaratory Judgment Act, 28 U.S.C. § 2201.

152. As previously alleged and pleaded, Defendant owed duties of care to Plaintiff and Class Members that required it to adequately secure their PII.

153. Defendant still possesses the PII of Plaintiff and the Class Members.

154. Defendant has not satisfied its obligations and legal duties to Plaintiff and the Class Members.

155. Green Diamond has claimed that it is taking some steps to increase its data security, but there is nothing to prevent Defendant from reversing these changes once it has weathered the increased public attention resulting from this Breach, and to once again place profits above protection.

156. Plaintiff, therefore, seeks a declaration (1) that Green Diamond's existing security measures do not comply with its obligations and duties of care to provide adequate security, and (2) that to comply with its obligations and duties of care, Defendant must implement and maintain reasonable security measures, including, but not limited to:

a. Ordering Defendant to engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant' systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

b. Ordering Defendant to significantly increase its spending on cybersecurity including systems and personnel;

TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53703-3515
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

c. Ordering Defendant to engage third-party security auditors and internal personnel to run automated security monitoring;

d. Ordering that Defendant audit, test, and train its security personnel regarding any new or modified procedures;

e. Ordering that Defendant segment Plaintiff's and the Class's PII by, among other things, creating firewalls and access controls so that if one area of Defendant' systems is compromised, hackers cannot gain access to other portions of Defendant's systems;

f. Ordering that Defendant cease storing unencrypted PII on its systems;

g. Ordering that Defendant conduct regular database scanning and securing checks;

h. Ordering Defendant to routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

i. Ordering Defendant to implement and enforce adequate retention policies for PII, including destroying, in a reasonably secure manner, PII once it is no longer necessary for it to be retained; and

j. Ordering Defendant to meaningfully educate its current, former, and prospective employees about the threats they face as a result of the loss of their financial and personal information to third parties, as well as the steps they must take to protect themselves.

VI. PRAYER FOR RELIEF

WHEREFORE, Plaintiff and the Class pray for judgment against Defendant as follows:

a. An order certifying this action as a class action under Fed. R. Civ. P. 23, defining the Class as requested herein, appointing the undersigned as Class

TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53703-3515
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

counsel, and finding that Plaintiff is a proper representative of the Class requested herein;

b. A judgment in favor of Plaintiff and the Class awarding them appropriate monetary relief, including compensatory damages, punitive damages, attorney fees, expenses, costs, and such other and further relief as is just and proper;

c. An order providing injunctive and other equitable relief as necessary to protect the interests of the Class as requested herein;

d. An order requiring Defendant to pay the costs involved in notifying the Class Members about the judgment and administering the claims process;

e. A judgment in favor of Plaintiff and the Class awarding them pre-judgment and post-judgment interest, reasonable attorneys' fees, costs and expenses as allowable by law; and

f. An award of such other and further relief as this Court may deem just and proper.

VII. DEMAND FOR JURY TRIAL

Plaintiff hereby demands a trial by jury on all appropriate issues raised in this Complaint.

Dated: April 30, 2024

Respectfully Submitted,

By: /s/ *Samuel J. Strauss*

Samuel J. Strauss (SBN 46971)
TURKE & STRAUSS LLP
613 Williamson St., Suite 201
Madison, WI 53703
Telephone: (608) 237-1775
Facsimile: (608) 509-4423
sam@turkestrauss.com

William B. Federman*
Kennedy M. Brian*
FEDERMAN & SHERWOOD
10205 North Pennsylvania Avenue
Oklahoma City, Oklahoma 73120

Telephone: (405) 235-1560
Facsimile: (405) 239-2112
wbf@federmanlaw.com
kpb@federmanlaw.com

pro hac vice request forthcoming

Counsel for Plaintiff and the Putative Class

TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53703-3515
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com